Adopt Ins 3700, to read as follows:

CHAPTER 3700 STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Statutory Authority: RSA 400-A:15 II.

PART Ins 3701 PURPOSE AND SCOPE

Ins 3701.01 Purpose and scope.

(a) This rule establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.

(b) Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards:

(1) To ensure the security and confidentiality of customer records and information;

(2) To protect against any anticipated threats of hazards to the security or integrity of such records; and

(3) To protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

(c) Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by rule with respect to persons engaged in providing insurance.

(d) Section 507 provides, among other things, that a state rule may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This rule requires that the safeguards established pursuant to this rule shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

PART Ins 3702 DEFINITIONS

Ins 3702.01 Definitions. For the purposes of this rule, the following definitions apply:

(a) "Customer" means a customer of the licensee as the term customer is defined in Ins 3001.04 (f).

(b) "Customer information" means nonpublic personal information as defined in Ins 3001.04 (s) about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

(c) "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

(d) "Licensee" means a licensee as that term is defined in Ins 3001.04 (q), except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the excess line business conducted pursuant to RSA 406-B.

(e) "Service provider" means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

PART Ins 3703 INFORMATION SECURITY PROGRAM

Ins 3703.01 Information Security Program. Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

PART Ins 3704 OBJECTIVES OF INFORMATION SECURITY PROGRAM

Ins 3704.01 Objectives. A licensee's information security program shall be designed to:

(a) Ensure the security and confidentiality of customer information;

(b) Protect against any anticipated threats or hazards to the security or integrity of the information; and

(c) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

PART Ins 3705 EXAMPLES OF METHODS OF DEVELOPMENT AND IMPLEMENTATION

Ins 3705.01 Examples. The actions and procedures described in Ins 3706 through Ins 3709 are examples of methods of implementation of the requirements of Ins 3703 and Ins 3704. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Ins 3703 and Ins 3704.

PART Ins 3706 ASSESS RISK

Ins 3706.01 Assess Risk. The licensee:

(a) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

(b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(c) Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

PART Ins 3707 MANAGE AND CONTROL RISK

Ins 3707.01 Manage and Control Risk. The licensee:

(a) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

(b) Trains staff, as appropriate, to implement the licensee's information security program; and

(c) Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

PART Ins 3708 OVERSEE SERVICE PROVIDER ARRANGEMENTS

Ins 3708.01 Oversee Service Provider Arrangements. The licensee:

(a) Exercises appropriate due diligence in selecting its service providers; and

(b) Requires its service providers to implement appropriate measurers designed to meet the objectives of this rule, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

PART Ins 3709 ADJUST THE PROGRAM

Ins 3709.01 Adjust the Program. The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes in customer information systems.

PART Ins 3710 DETERMINED VIOLATION

Ins 3710.01 Violations. Violations of any of the provisions of this rule shall be **[considered violations of RSA 417 and]** subject to the penalties **of RSA 400-A:15 III [thereunder]**.

PART Ins 3711 EFFECTIVE DATE

Ins 3711.01 Effective Date. Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this rule **6 months after the effective date of this rule [by December 1, 2002]**.

(ins3700fpat082503.doc)